FICHE TECHNIQUE

Zscaler™ Cloud Sandbox

Protection intelligente contre le patient zéro

Zscaler Cloud Sandbox est bâti sur une architecture révolutionnaire basée sur un proxy pour la détection, la neutralisation et la mise en quarantaine en ligne des attaques inconnues, notamment les menaces dissimulées dans le trafic TLS/SSL. Piloté par l'IA/ML avancée, Cloud Sandbox bloque les attaques dites patient zéro grâce à des analyses instantanées pour les types de fichiers courants et la mise en quarantaine automatique pour les menaces inconnues à haut risque.

Quand avez-vous pour la dernière fois lancé un logiciel client de messagerie pour vérifier votre e-mail ? Les choses ont changé. Les entreprises adoptent rapidement la transformation digitale pour répondre à la forte demande d'applications SaaS, de charges de travail du cloud public et d'accès à distance, lesquels ont considérablement augmenté et ouvert de nouvelles surfaces d'attaque pour les entreprises dont les infrastructures de réseau sont basées sur le modèle cloisonné d'antan. Les hackers modernes le savent et en tirent parti en concevant et en lançant des attaques automatisées et hautement ciblées qui contournent facilement les défenses traditionnelles contre les logiciels malveillants centrées sur le réseau, ce qui se traduit souvent par des infections de type patient zéro.

Du coup, les leaders des services informatiques et de la sécurité se trouvent confrontés à un dilemme : les réseaux cloisonnés sont passés de mode, les utilisateurs et les données sont partout, et la surface d'attaque continue de s'étendre. Ils ont réalisé que les approches de type passthrough basées sur des appliances/sandbox hors bande ne sont plus appropriées. Leurs résultats en matière de sécurité ont un effet inverse. Au lieu de garder une longueur d'avance sur les hackers en préservant une solide posture de sécurité, ils doivent faire face à :

Un contrôle réactionnel des dégâts

Les sandbox hors bande et basés sur des appliances sont conçus pour les réseaux traditionnels cloisonnés. Leur architecture de type passthrough permet au premier fichier inconnu et potentiellement malveillant de passer sans inspection approfondie ni mise en quarantaine, ce qui se traduit souvent par des infections de type patient zéro. En conséquence, les leaders de la sécurité et de l'informatique se retrouvent obligés de combattre le mouvement latéral de logiciels malveillants inconnus, ce qui aurait dû être évité dès le départ. Ils continuent de déployer des protections supplémentaires à l'intérieur de leurs réseaux et de créer des règles complexes de segmentation du réseau sur leurs anciens pare-feux virtuels et basés sur des appliances, ce qui augmente leurs coûts opérationnels. Pour mettre les choses en perspective, en 2017, une attaque historique sur Maersk a complètement arrêté une entreprise de 80 000 employés en seulement trois heures et a causé des milliards de dollars de dommages[1].

AVANTAGES POUR LES LEADERS DE LA SÉCURITÉ

- **Véritable protection inline :** détecter, empêcher et mettre en quarantaine les menaces inconnues inline grâce à une IA/ML avancée pour mettre en échec les attaques de type patient zéro.
- **Visibilité SSL complète :** identifier les menaces inconnues dans tout le trafic TLS/SSL grâce à une architecture unique basée sur proxy qui permet une inspection fluide et illimitée.
- **Protection systématique partout :** protection fournie dans le cloud pour chaque utilisateur, quel que soit son emplacement. Tout le monde bénéficie de la même protection sur le réseau ou en dehors, sans VPN encombrants ni liens MPLS onéreux.
- **Prévention partagée à l'échelle mondiale :** bénéficier d'une protection automatisée contre les menaces inconnues grâce au partage en temps réel avec tous les utilisateurs, des renseignements intégrés sur les menaces.
- **Réduction de la complexité et du TCO :** éliminer la complexité et déployer en quelques secondes, sans matériel à acheter ni logiciel à gérer. Cloud Sandbox est une fonctionnalité entièrement intégrée de Zscaler Internet Access™, qui fait partie de Zscaler Zero Trust Exchange™.

[1] https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/

De persistants problèmes d'administration

En moyenne, une entreprise déploie 45 outils de sécurité différents[2] dans son réseau pour se protéger contre les cyberattaques. L'ajout de sandbox basés sur des appliances ou de solutions hors bande qui reposent sur une autre appliance pour exécution n'a pas de sens. De plus, il est contre-productif pour les leaders de la sécurité et des services informatiques de gérer les projets de transformation digitale en cours tout en s'occupant des mises à niveau matérielles, des correctifs, des politiques exagérées, de la segmentation du réseau, des protocoles de routage et d'interminables appels d'assistance. Dans un environnement réseau traditionnel, le service informatique consacre la plupart de son temps à résoudre les problèmes plutôt que de consolider la posture de sécurité de l'entreprise.

Un manque de visibilité

Quatre-vingt-quatre pour cent du trafic Internet mondial est chiffré via SSL/TLS, ce chiffre approchant rapidement les 92 % aux États-Unis[3]. Les hackers y voient une aubaine et lancent des attaques furtives dissimulées dans le trafic crypté. Un récent rapport de ThreatLabZ a révélé une augmentation de 500 % des attaques de ransomware dissimulées dans le trafic SSL et, fait intéressant, on a observé que 30 % des applications cloud fiables comme Google Drive, AWS et OneDrive diffusaient des logiciels malveillants. Les sandbox centrés sur le réseau ne sont pas conçus pour inspecter le trafic SSL, ce qui les rend inutiles lorsqu'il s'agit de détecter des attaques inconnues furtives et ciblées.

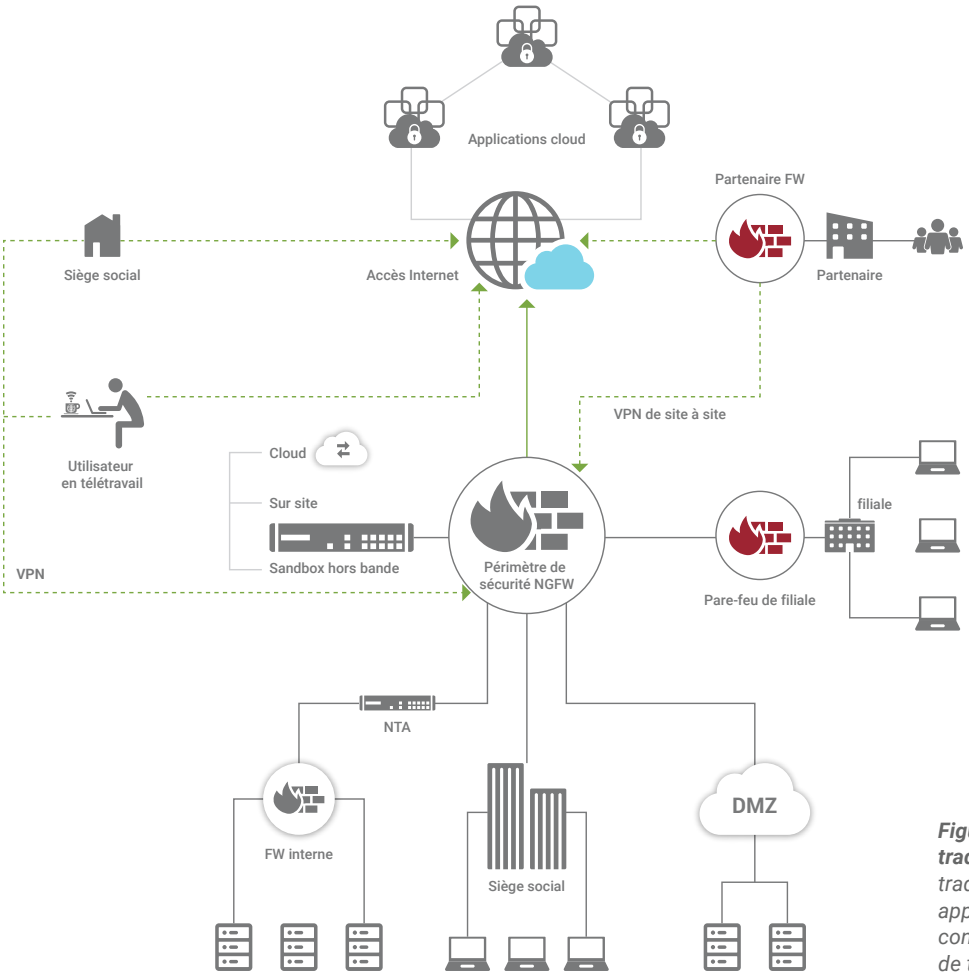

Figure 1 : architecture traditionnelle : *Sandbox traditionnel basé sur des appliances et hors bande, conçu pour les réseaux de type cloisonné*

[2] https://www.zdnet.com/article/the-more-cybersecurity-tools-an-enterprise-deploys-the-less-effective-their-defense-is/
[3] https://www.abetterinternet.org/documents/2020-ISRG-Annual-Report.pdf

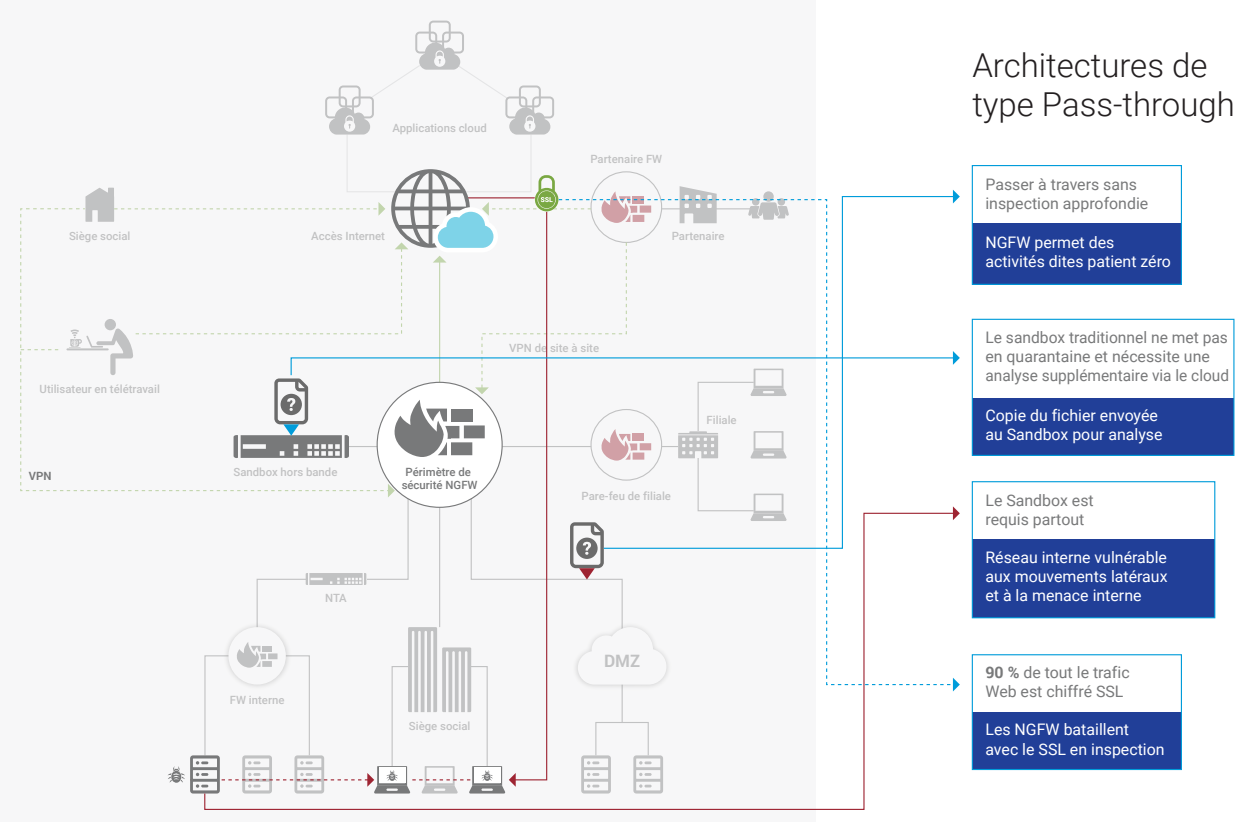

Figure 2 : infection du type patient zéro : *l'architecture de type passthrough du sandbox traditionnel laisse passer n'importe quel fichier potentiellement malveillant*

L'approche Zero Trust de Zscaler avec le sandbox Cloud-Gen

Zscaler Cloud Sandbox est bâti sur Zscaler Zero Trust Exchange™, une plateforme basée sur une architecture proxy spécialement conçue et unique. Zero Trust Exchange utilise un moteur d'analyse des données alimenté par IA/ML qui permet la détection en ligne, la neutralisation et la mise en quarantaine basée sur l'IA des attaques inconnues, notamment les menaces dissimulées dans le trafic SSL/TLS.

Piloté par l'IA/ML avancée, Cloud Sandbox bloque les attaques dites patient zéro grâce à des analyses instantanées pour les types de fichiers courants et la mise en quarantaine automatique pour les menaces inconnues à haut risque. En tant que service intégré de la plateforme Zscaler native du cloud, les protections sont en permanence mises à jour à partir de plus de 160 milliards de requêtes au quotidien.

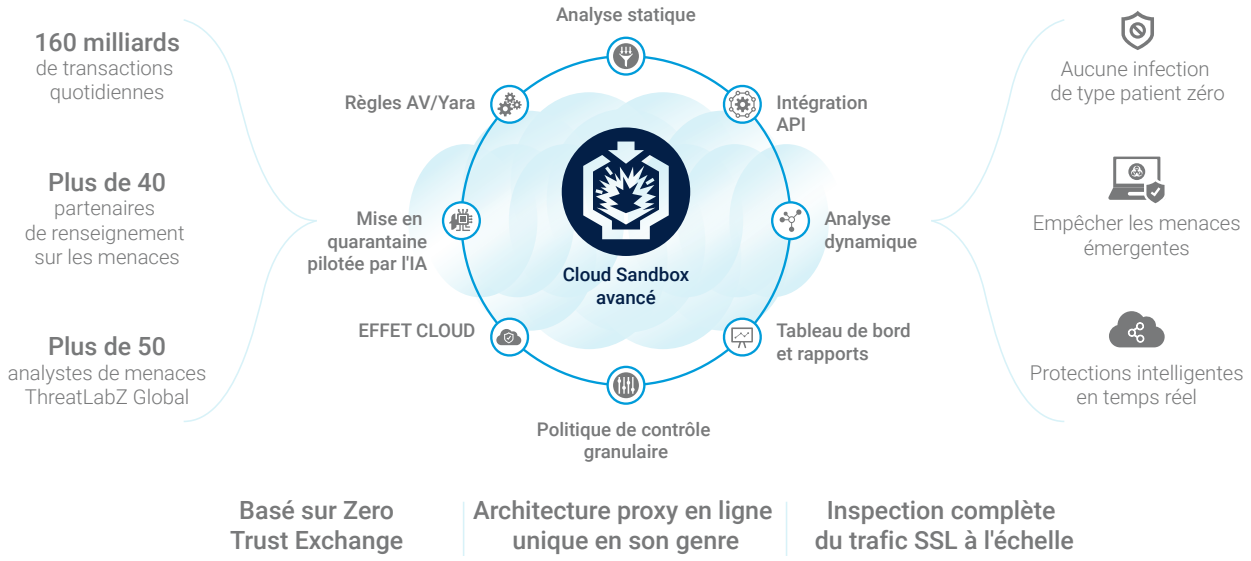

Figure 3 : *Zscaler Advanced Cloud Sandbox*

Être proactif

L'architecture proxy inline de Zscaler permet aux équipes de sécurité d'être plus proactives dans la neutralisation des menaces de type patient zéro. L'architecture native du cloud permet une inspection illimitée de tout le trafic sur tous les ports et protocoles, y compris le trafic SSL/TLS. Grâce à la première fonctionnalité de quarantaine basée sur l'IA du secteur, associée à un moteur d'analyse dynamique approfondi, vous pouvez désormais détecter, inspecter, donner l'alerte et bloquer de manière proactive les fichiers inconnus suspects et potentiellement dangereux avant qu'ils n'intègrent le réseau. En outre, en fonction de votre cas d'utilisation souhaité, vous pouvez créer et déployer des politiques sandbox granulaires basées sur les utilisateurs et les applications sans avoir besoin de paramètres de configuration de réseau traditionnels.

S'affranchir des appliances et des sandbox hors bande

Zscaler Cloud Sandbox est fourni à 100 % dans le cloud. Il n'est pas nécessaire de recourir à des appliances ou à une analyse sandbox hors bande. Libérez-vous d'incessantes mises à niveau d'appliances, de la poursuite des fenêtres de changement, du stockage et de l'empilage des appliances, de la gestion des protocoles de routage, du backhauling de trafic vers les appliances réseau, de médiocres expériences utilisateur et de l'ajout d'éléments supplémentaires à une politique déjà surchargée. Zscaler permet de configurer facilement le sandbox, le rendant opérationnel en quelques secondes.

Obtenir une inspection SSL illimitée

L'architecture proxy inline de Zscaler, unique en son genre, vous permet d'inspecter le trafic SSL/TLS à une échelle illimitée et de neutraliser les menaces cachées. Étant donné que la majorité du trafic Internet et des applications utilisent SSL comme canal de communication, vous avez besoin d'une solution capable d'inspecter et de détecter les menaces émergentes dissimulées dans le trafic chiffré sans compromettre l'expérience utilisateur.

Garder une longueur d'avance sur les hackers

Zscaler exploite la puissance du cloud en fournissant des politiques de sandbox recommandées qui se mettent automatiquement à jour avec les dernières protections partagées provenant de nouvelles menaces découvertes par notre sandbox. Avec plus de 160 milliards de transactions traitées au quotidien, une équipe de chercheurs en menaces de classe mondiale et des informations sur sept milliards de menaces bloquées dans le cloud, les utilisateurs sont toujours protégés sur le réseau ou en dehors.

Moteur d'analyse dynamique approfondie des programmes malveillants

Le moteur d'analyse dynamique approfondie Zscaler Cloud Sandbox tire pleinement parti du cloud en vérifiant les hachages par rapport à une liste noire provenant de flux de menaces et d'autres échantillons observés — en pré-filtrant les échantillons pour optimiser l'analyse et en fournissant rapidement des verdicts avec des modèles AV, Yara et AI/ML. De robustes pipelines d'analyse statique, dynamique et secondaire produisent rapidement des verdicts exploitables. Le post-traitement continue à mettre à jour la base de données des menaces de Zscaler et à actualiser les politiques appliquées par les clients, même une fois l'analyse terminée.

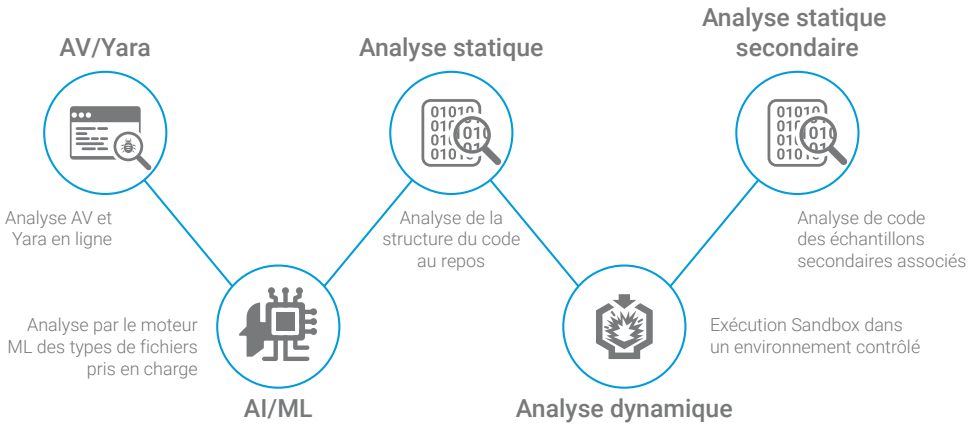

Figure 4 : *flux d'analyse des menaces de Zscaler Advanced Cloud Sandbox*

Caractéristiques principales de Zscaler Cloud Sandbox

Configuration facile 1-2

Vous n'avez besoin ni d'utiliser plusieurs fenêtres pour gérer, ni d'appliances à déployer. Rendez Zscaler Cloud Sandbox opérationnel en quelques secondes grâce à une configuration simple en deux étapes : critères et action.

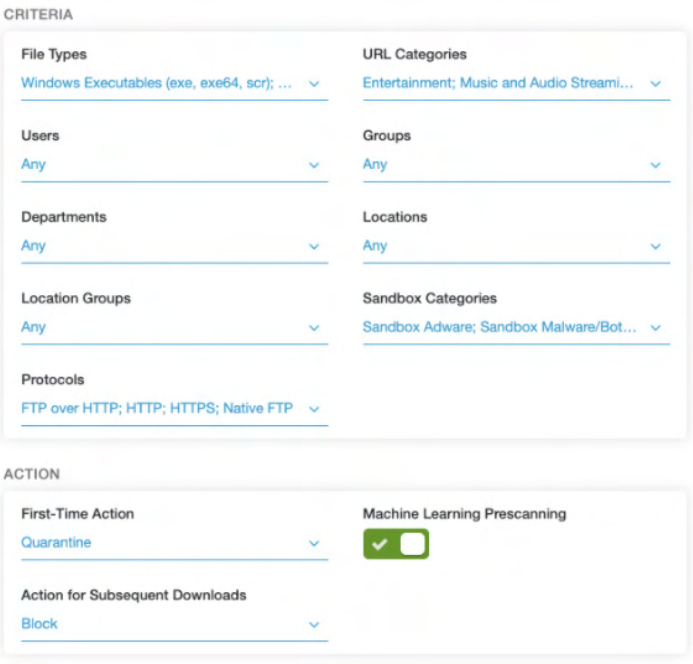

Figure 5 : *configuration facile de la politique de Zscaler Advanced Cloud Sandbox*

Politiques granulaires

Créer des politiques personnalisées et granulaires pour prendre en charge différents cas d'utilisation, prendre des mesures en conservant les fichiers pour une mise en quarantaine basée sur l'IA et fournir un accès en fonction des utilisateurs, de l'emplacement, du système d'exploitation et d'autres paramètres.

Figure 6 : *contrôle granulaire de la politique de Zscaler Advanced Cloud Sandbox*

Quarantaine basée sur l'IA

Neutraliser les infections de type patient zéro avant qu'elles n'atteignent leur cible. L'architecture proxy de Zscaler vous permet de mettre en quarantaine les fichiers suspects inline, d'effectuer en temps réel des analyses basées sur l'IA et de rendre sans délai des verdicts instantanés.

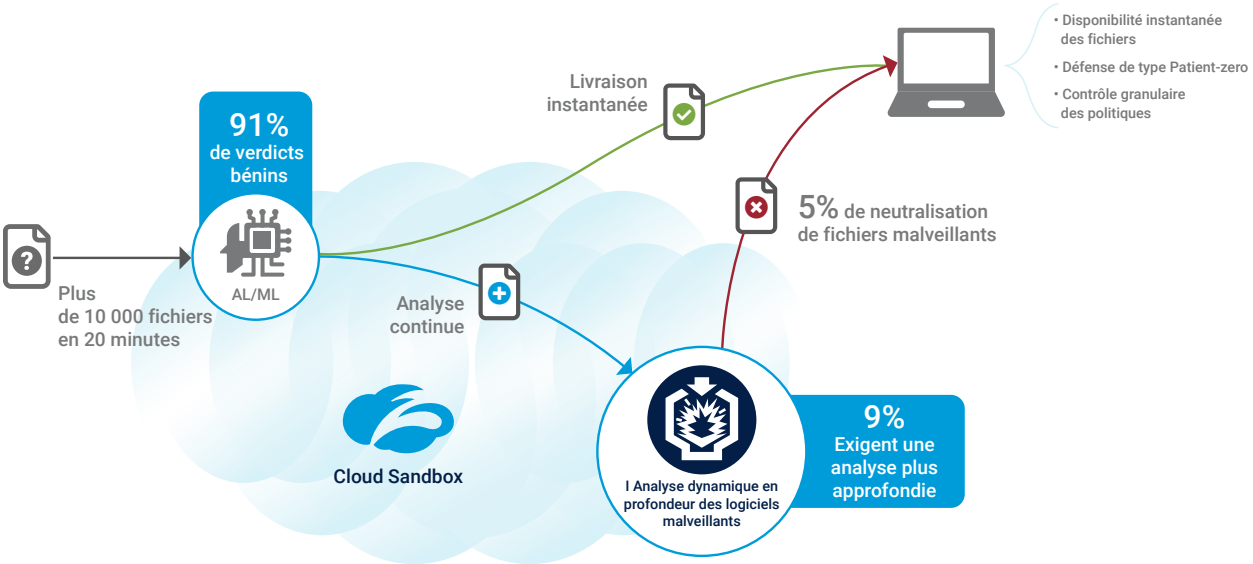

Figure 7 : *flux d'analyse de quarantaine basé sur l'IA de Zscaler Advanced Cloud Sandbox*

L'IA en action : dans les vingt minutes qui ont suivi le déploiement, un client qui utilisait Zscaler Cloud Sandbox a vu 91 % des fichiers inconnus obtenir un verdict bénin instantané basé sur l'IA avant d'être rapidement transmis aux utilisateurs. Les neuf pour cent de fichiers restants ont fait l'objet d'une analyse dynamique et approfondie qui a révélé que cinq pour cent des fichiers étaient malveillants. Ces fichiers dangereux ont été grâce à l'effet cloud instantanément bloqués pour tous les utilisateurs de Zscaler à travers le monde.

Rapports détaillés

Des rapports approfondis sur les verdicts émis permettent aux équipes d'opérations de sécurité d'accélérer les investigations tout comme la chasse aux menaces, permettant aux leaders de la sécurité de renforcer rapidement la sécurité.

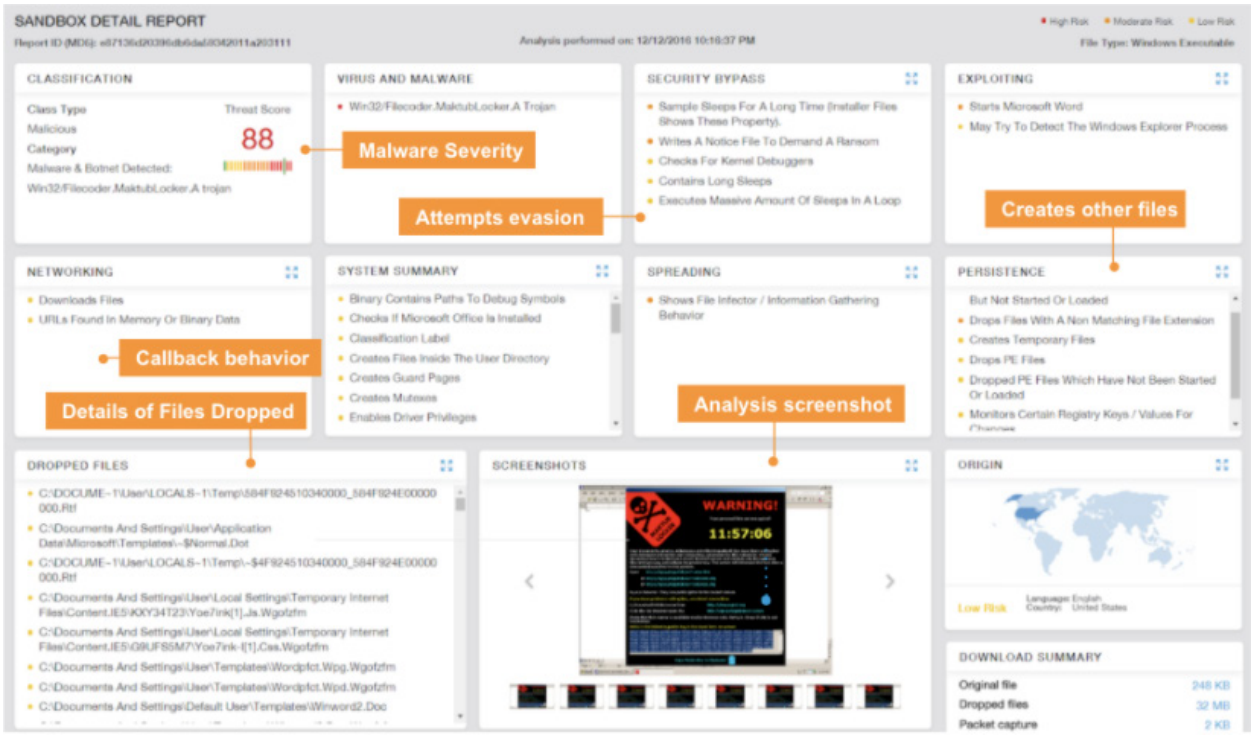

Figure 8 : *rapport légal détaillé de Zscaler Advanced Cloud Sandbox*

Caractéristiques de Cloud Sandbox

Fonctions	Détails
Moteur d'analyse	Pré-filtrage : AV, Yara, ML/AI ; Analyse : analyse statique, analyse dynamique ; Post analyse : analyse du code, analyse des charges utiles secondaires
Prise en charge des fichiers	.exe, .dll, .scr, .ocx, .sys, .class, .jar, .pdf, .swf, Documents Office, .apk, .zip, .rar, .7z, .bz, .bz2, .tar, .tgz, .gtar, .rtf, .ps1, .hta, .vba, fichiers script dans zips
Inspection SSL	Inspection SSL/TLS illimitée
Prise en charge du système d'exploitation	Windows XP, Windows 10 et Android
Prise en charge du protocole	HTTP, HTTPS, FTP, FTP à travers HTTP
Fichiers par jour	Illimité
Modèle de déploiement	Natif du Cloud
Intégration des renseignements sur les menaces	Plus de 40 flux d'informations sur les menaces des partenaires de sécurité
Gestion et rapport	Interface utilisateur Web centralisée
Légal	Échantillon initial, charges utiles secondaires, PCAP
Prise en charge des API	Prise en charge robuste de l'API
Politiques granulaires	Utilisateurs, emplacement, groupes de localisations, types de fichiers, groupes d'utilisateurs, services, catégories d'URL, protocoles

Conditions préalables :

- Nécessité de disposer d'une licence de protection contre les menaces avancées (ATP) et de déchiffrement SSL

Modèle de licence de Zscaler :

- ZIA Professional Edition : inclut Cloud Sandbox Standard
- ZIA Business Edition : comprend le Cloud Sandbox standard, la protection contre les menaces avancées (ATP) et le déchiffrement SSL
- ZIA Transformation Edition : inclut le Cloud Sandbox avancé, la protection avancée contre les menaces (ATP) et le déchiffrement SSL

Zscaler Cloud Sandbox en tant que module complémentaire

- ZIA-Sandbox : nécessite une licence Business ou Professional Edition

	Sandbox cloud standard	Cloud Sandbox avancé
Prise en charge des fichiers	.exe, .dll,	.exe, .dll, .scr, .ocx, .sys, .class, .jar, .pdf, .swf, Documents de bureau Zcs,.doc(x), .xls(x), .ppt(x), .apk, .zip, .rar, .7z, .bz, .bz2, .tar, .tgz, .gtar, .rtf, .ps1, .hta, .vba, fichiers script dans zips
Quarantaine basée sur l'IA	✗	✓
Politiques granulaires	✗	✓
Reporting	✗	✓
API	✗	✓

Obtenez plus de détails sur notre cloud sandbox avancé en visitant le site **https://www.zscaler.fr/technology/cloud-sandbox**

Faites un essai virtuel de notre cloud sandbox avancé en vous inscrivant aux **« Ateliers pratiques de Zscaler »**

À propos de Zscaler
Zscaler (NASDAQ: ZS) accélère la transformation digitale de sorte que les clients deviennent plus agiles, plus efficaces, plus résilients et plus en sécurité. La plateforme Zscaler Zero Trust Exchange protège des milliers de clients contre les cyberattaques et la perte des données en connectant de manière sécurisée les utilisateurs, les appareils et les applications indépendamment de l'emplacement. Distribué à travers plus de 150 data centers dans le monde, Zero Trust Exchange basé sur SASE est la plus grande plateforme de sécurité cloud inline. Pour en savoir plus, rendez-vous sur **zscaler.com** ou suivez-nous sur Twitter **@zscaler**.

Zscaler, Inc.
120 Holger Way
San José, Californie
+1 408 533 0288
www.zscaler.com